CLAIMS

What is claimed is:

1. A method of providing security for a computer system, the method comprising the acts of:

generating a request for a file;

receiving the request at a dedicated security processor;

using the dedicated security processor to access the file;

using the dedicated security processor to validate the requested file; and

providing the file to an other processor, if the requested file is validated.

2. The method, as set forth in claim 1, comprising the act of validating a user access to execute the request.

3. The method, as set forth in claim 2, comprising the act of responding to the other processor with an abort message if the user access is invalid.

4. The method, as set forth in claim 2, comprising the act of enabling the other processor to continue processing the file, if the user access is validated.

5. The method, as set forth in claim 1, comprising the act of disabling the other processor once the file is requested and enabling the other processor to continue processing after the requested file is validated.

6. The method, as set forth in claim 1, wherein accessing the file comprises loading the file from a system memory.

7. The method, as set forth in claim 1, wherein accessing the file comprises loading a memory resident file.

8. The method, as set forth in claim 1, wherein the dedicated security processor is in a remote computer system.

9. The method, as set forth in claim 1, wherein the other processor and the dedicated security processor are disposed in a computer system.

10. The method, as set forth in claim 1, comprising the act of setting a return status field to valid, if the requested file is valid.

11. The method, as set forth in claim 1, wherein the act of generating the request comprises the acts of:

setting a semaphore;

forwarding the semaphore to the dedicated security processor; and

blocking further processing of the file, if the semaphore is not set to a specific setting.

12. The method, as set forth in claim 1, wherein the act of validating the requested file comprises the act of accessing a database for a digital signature of the file being requested.

13. The method, as set forth in claim 12, wherein the act of validating the requested file comprises the act of calculating a secure hash and comparing the calculated secure hash to a stored secure hash.

14. The method, as set forth in claim 1, wherein the act of validating the requested file comprises the act of accessing a database for an error checking and correction ("ECC") code corresponding to the requested file.

15. The method, as set forth in claim 14, wherein the act of accessing the database comprises the act of correcting the file by utilizing the ECC code corresponding to the requested file.

16. A method of providing security for a computer system, the method comprising the acts of:

generating an identifying number from a security processor;

providing the identifying number to an other processor in the computer system;

incorporating the identifying number into a request for a file;

delivering the request to the security processor;

using the security processor to access the file;

using the security processor to validate the requested file;

verifying the identifying number at the security processor; and

providing the file, if the requested file is validated and the identifying number is verified.

17. The method, as set forth in claim 16, comprising the act of enabling the other processor to continue the processing, if the identifying number is validated.

18. The method, as set forth in claim 16, comprising the act of terminating the access if the identifying number is invalid.

19. The method, as set forth in claim 16, wherein the security processor is in a remote computer system.

20. The method, as set forth in claim 16, wherein the other processor and the security processor are disposed in the computer system.

21. The method, as set forth in claim 16, wherein the identifying number is a nonce.

22. The method, as set forth in claim 16, wherein the identifying number is a time stamp.

23. The method, as set forth in claim 16, wherein the act of validating the requested file comprises the act of accessing a database for an error checking and correction ("ECC") code corresponding to the requested file.

24. A computer system comprising:

means for validating a file at a security processor, wherein the means for validating the file comprises:

means for storing a record in a memory used to validate the file;

means for verifying the record against the file at the security processor; and

means for indicating that the file is verified to an other processor.

25. The system, as set forth in claim 24, comprises means for validating a user access.

26. The system, as set forth in claim 24, wherein the means for verifying comprises:

means for storing a public key and a hash algorithm used to validate the file;

means for storing an encrypted hash correlative to the requested file in the record; and

means for comparing the record with the requested file.

27. The system, as set forth in claim 24, comprises means for verifying an identifying number in a request at the security processor.

28. A networked computer system comprising:

a plurality of computer systems;

a network coupled to each of the plurality of computer systems;

at least one of the plurality of computer systems comprising:

a first processor;

a security processor operatively coupled to the first processor;

a first section of memory configured to store a file, the first section of memory being operatively coupled to the first processor and the security processor; and

a second section of memory being configured to store a validation program that is initiated by the security processor, the validation program having a validation routine configured to validate the file stored in the first section of memory when the security processor receives a request for the file, and the validation program using an encrypted code to validate the file.

29. The system, as set forth in claim 28, wherein a second processor in a second of the plurality of computer systems is adapted to utilize the security processor for validating the file.

30. The system, as set forth in claim 29, wherein the memory is a memory resident file.

31. The system, as set forth in claim 28, wherein the request comprises a semaphore and an address for the semaphore, wherein the semaphore blocks the processor from executing the file, if the semaphore is set in a specified manner.

32. The system, as set forth in claim 28, wherein a second processor in a second of the plurality of computer systems is adapted to generate a request for the file from the security processor and is adapted to receive the validated file from the security processor.